

#2

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

JC846 U.S. PTO
09/765365
01/22/01

January 22, 2001

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Kotaro NAGAHAMA
TERMINAL CERTIFICATION SYSTEM AND
METHOD OF CERTIFYING THE SAME
Our Ref. Q62489

Dear Sir:

Attached hereto is the application identified above including 25 sheets of the specification, including the claims and abstract, 11 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney.

The Government filing fee is calculated as follows:

Total claims	16	-	20	=		x	\$18.00	=	\$0.00
Independent claims	3	-	3	=		x	\$80.00	=	\$0.00
Base Fee									\$710.00
TOTAL FILING FEE									\$710.00
Recordation of Assignment									\$40.00
TOTAL FEE									\$750.00

Checks for the statutory filing fee of \$710.00 and Assignment recordation fee of \$40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from January 25, 2000 based on Japanese Application No. 2000-15670. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: J. Frank Osha
J. Frank Osha
Registration No. 24,625

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

K. Nagahama

1/22/01

Q 62489

1 of 1



1c846 U.S. PTO
09/765365

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 1月25日

出願番号

Application Number:

特願2000-015670

出願人

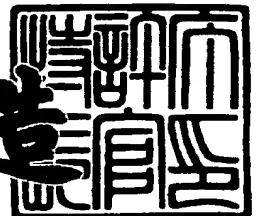
Applicant(s):

日本電気株式会社

2000年11月17日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3095562

【書類名】 特許願

【整理番号】 66400347

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 永浜 公太郎

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【手数料の表示】

【予納台帳番号】 008279

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

()

特 2 0 0 0 - 0 1 5 6 7 0

【包括委任状番号】 9115699

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証システムおよびその方法

【特許請求の範囲】

【請求項 1】 複数の端末と、これら複数の端末が接続される接続装置とを有して構成される認証システムであって、

前記接続装置および前記複数の端末のそれぞれは、時間に応じてパスワードを変更するパスワードコントローラを有し、

前記接続装置は、前記端末のパスワードコントローラで生成されたパスワードと前記接続装置のパスワードコントローラで生成されたパスワードとが一致する際に、該端末の通信を許可することを特徴とする認証システム。

【請求項 2】 前記パスワードコントローラは、複数のパスワードを格納するパスワード格納メモリと、

このパスワード格納メモリに格納された複数のパスワードから 1 つを選択するパスワード選択回路とを有し、

前記パスワード選択回路は、時間に応じてパスワードの選択を変更することを特徴とする請求項 1 記載の認証システム。

【請求項 3】 前記パスワードコントローラはさらにタイマと、

時刻によっていずれのパスワードを使用するかを示す設定情報を格納する設定メモリとを有し、

前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード選択回路は、前記タイマの示す時間および前記設定情報に従ってパスワードの選択を変更することを特徴とする請求項 2 記載の認証システム。

【請求項 4】 前記接続装置は、前記ネットワークとのフレームの送受信を行うフレーム転送処理部と、

前記端末と接続されて前記端末とフレームの送受信を行う複数のインタフェースと、

前記端末から送信されてくるフレームのパスワードと、前記接続装置の前記パ

スワードコントローラで選択されたパスワードとを比較するパスワード比較器とをさらに有し、

前記インタフェースは、前記パスワード比較器がパスワードの一致を示した場合、対応するフレームを前記フレーム転送処理部へ転送し、不一致を示した場合、対応するフレームを廃棄することを特徴とする請求項 1 記載の認証システム。

【請求項 5】 前記複数の端末はそれぞれ、前記接続装置とのフレームの送受信を制御するフレーム送受信部と、

前記接続装置にフレームを送信する場合に、前記パスワードコントローラからパスワードを受け取り、該パスワードをフレームに付加するフレーム組立部をさらに有することを特徴とする請求項 3 記載の認証システム。

【請求項 6】 前記フレーム組立部は、前記パスワードコントローラからさらにパスワード選択時間を受け取り、前記接続装置に送信するフレームに該パスワードおよびパスワード選択時間を付加することを特徴とする請求項 5 記載の認証システム。

【請求項 7】 前記接続装置のパスワードコントローラは所定の有効時間を格納した有効時間格納メモリをさらに有し、

前記パスワード選択部は、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以内であれば前記パスワード選択時間と前記設定情報とから使用するパスワードを選択し、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以上であれば前記タイマの示す時刻と前記設定情報とから使用するパスワードを選択することを特徴とする請求項 6 記載の認証システム。

【請求項 8】 前記パスワードコントローラは、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリと、

このアルゴリズム格納メモリに格納された複数のパスワード生成アルゴリズムから 1 つを選択してパスワードを生成するパスワード生成回路とを有し、

前記パスワード生成回路は、時間に応じてパスワード生成アルゴリズムを変更してパスワードを生成することを特徴とする請求項 1 記載の認証システム。

【請求項 9】 前記パスワードコントローラはさらにタイマと、時刻によっていずれのパスワード生成アルゴリズムを使用するかを示す設定情

報を格納する設定メモリとを有し、

前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード生成回路は、前記タイマの示す時間および前記設定情報に従ってパスワード生成アルゴリズムを選択してパスワードを生成することを特徴とする請求項 8 記載の認証システム。

【請求項 1 0】 前記複数のパスワード生成アルゴリズムのそれぞれは、前記タイマの示す時刻に従って異なるパスワードを生成することを特徴とする請求項 8 記載の認証システム。

【請求項 1 1】 複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれが時間に応じてパスワードを変更するパスワードコントローラを有するシステムの認証方法であって、

前記接続装置と前記端末との時間を同期させ、

前記端末は、フレームを送信する際に当該端末の前記パスワードコントローラが時間に応じて選択したパスワードをフレームに付加して前記接続装置に送信し

、
前記接続装置は、受け取ったフレームに付加されたパスワードと、前記接続装置の前記パスワードコントローラが時間に応じて選択したパスワードとを比較し

、
パスワードが一致すれば当該フレームの送信を許可し、一致しなければ当該フレームの送信を許可せず当該フレームを廃棄することを特徴とする認証方法。

【請求項 1 2】 前記端末は、フレームを前記接続装置に送信する際に、フレームに対して当該端末の前記パスワードコントローラがパスワードを選択した選択時間をさらに付加し、

前記接続装置の前記パスワードコントローラは、前記選択時間に応じてパスワードを選択することを特徴とする請求項 1 1 記載の認証方法。

【請求項 1 3】 前記パスワードコントローラは、時間に応じて複数のパスワード生成アルゴリズムの中から 1 つを選択し、該パスワード生成アルゴリズム

によりパスワードを生成することを特徴とする請求項 1 1 記載の認証方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、システムに接続される端末の認証システムおよびその方法に関する

【0 0 0 2】

【従来の技術】

従来のシステムは、図 1 7 に示されるように、LAN (Local Area Network) などのネットワーク 4 に接続された接続装置 1 に複数の端末 2 が接続されて構築されている。この従来のシステムでは、ネットワーク 4 にアクセス可能な端末の送信元アドレスを管理者があらかじめ接続装置 1 に登録していた。そして、接続装置 1 は、登録された送信元アドレスと端末 2 から送信されてくるフレームの送信元アドレスとを照合することで、当該端末が管理者の許可を受けた端末かどうかを区別していた。

【0 0 0 3】

また、従来の他のシステムでは、接続装置 1 と端末 2 との双方に特定のパスワードを持たす構成にしていた。この従来の他のシステムでは、まず、端末が特定のパスワードを付加したフレームを送信する。接続装置 1 は、同じ特定のパスワードと端末 2 から受け取ったフレームのパスワードとを照合することで端末 2 のネットワーク 4 への接続の可否を判断していた。

【0 0 0 4】

【発明が解決しようとする課題】

しかしながら、上述の従来技術では、侵入者が許可された送信元アドレスやパスワードを盗用することにより、あたかも管理者から許可を受けた端末 2 であるかのように見せかけて接続装置 1 に端末 2 を接続する恐れがあった。このような場合、接続装置 1 はその端末 2 が正しく許可されているものと判断してしまう。このため、不正に接続した端末 2 がネットワーク 4 を介して他の端末と通信が成立してしまい、セキュリティが保たれなくなるという問題点があった。

【 0 0 0 5 】

本発明の目的は、このような送信元アドレスやパスワードの盗用による不正アクセスを検出して排除できるセキュリティの高い認証システムを提供することにある。

【 0 0 0 6 】

【課題を解決するための手段】

上記課題を解決するために本発明の認証システムは、複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれは、時間に応じてパスワードを変更するパスワードコントローラを有し、前記接続装置は、前記端末のパスワードコントローラで生成されたパスワードと前記接続装置のパスワードコントローラで生成されたパスワードとが一致する際に、該端末の通信を許可する。

【 0 0 0 7 】

また、前記パスワードコントローラは、複数のパスワードを格納するパスワード格納メモリと、このパスワード格納メモリに格納された複数のパスワードから1つを選択するパスワード選択回路とを有し、前記パスワード選択回路は、時間に応じてパスワードの選択を変更する。

【 0 0 0 8 】

さらに、前記パスワードコントローラはさらにタイマと、時刻によっていずれのパスワードを使用するかを示す設定情報を格納する設定メモリとを有し、前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード選択回路は、前記タイマの示す時間および前記設定情報に従ってパスワードの選択を変更する。

【 0 0 0 9 】

また、前記接続装置は、前記ネットワークとのフレームの送受信を行うフレーム転送処理部と、前記端末と接続されて前記端末とフレームの送受信を行う複数のインタフェースと、前記端末から送信されてくるフレームのパスワードと、前記接続装置の前記パスワードコントローラで選択されたパスワードとを比較する

パスワード比較器とをさらに有し、前記インタフェースは、前記パスワード比較器がパスワードの一致を示した場合、対応するフレームを前記フレーム転送処理部へ転送し、不一致を示した場合、対応するフレームを廃棄する。

【 0 0 1 0 】

さらに、前記複数の端末はそれぞれ、前記接続装置とのフレームの送受信を制御するフレーム送受信部と、前記接続装置に送信するフレーム毎に、前記パスワードコントローラからパスワードを受け取り、該パスワードをフレームに付加するフレーム組立部をさらに有する。

【 0 0 1 1 】

また、前記フレーム組立部は、前記パスワードコントローラからさらにパスワード選択時間を受け取り、前記接続装置に送信するフレームに該パスワードおよびパスワード選択時間を付加する。

【 0 0 1 2 】

さらに、前記接続装置のパスワードコントローラは所定の有効時間を格納した有効時間格納メモリをさらに有し、前記パスワード選択部は、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以内であれば前記パスワード選択時間と前記設定情報とから使用するパスワードを選択し、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以上であれば前記タイマの示す時刻と前記設定情報とから使用するパスワードを選択する。

【 0 0 1 3 】

また、前記パスワードコントローラは、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリと、このアルゴリズム格納メモリに格納された複数のパスワード生成アルゴリズムから1つを選択してパスワードを生成するパスワード生成回路とを有し、前記パスワード生成回路は、時間に応じてパスワード生成アルゴリズムを変更してパスワードを生成する。

【 0 0 1 4 】

さらに、前記パスワードコントローラはさらにタイマと、時刻によっていずれのパスワード生成アルゴリズムを使用するかを示す設定情報を格納する設定メモリとを有し、前記端末の前記パスワードコントローラの前記タイマは、前記端末

が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード生成回路は、前記タイマの示す時間および前記設定情報に従ってパスワード生成アルゴリズムを選択してパスワードを生成する。

【0015】

また、前記複数のパスワード生成アルゴリズムのそれぞれは、前記タイマの示す時刻に従って異なるパスワードを生成する。

【0016】

さらに、本発明における認証方法は、複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれが時間に応じてパスワードを変更するパスワードコントローラを有するシステムの認証方法であって、前記接続装置と前記端末との時間を同期させ、前記端末は、フレームを送信する際に当該端末の前記パスワードコントローラが時間に応じて選択したパスワードをフレームに付加して前記接続装置に送信し、前記接続装置は、受け取ったフレームに付加されたパスワードと、前記接続装置の前記パスワードコントローラが時間に応じて選択したパスワードとを比較し、パスワードが一致すれば当該フレームの送信を許可し、一致しなければ当該フレームの送信を許可せず当該フレームを廃棄する。

【0017】

また、前記端末は、フレームを前記接続装置に送信する際に、フレームに対して当該端末の前記パスワードコントローラがパスワードを選択した選択時間をさらに付加し、前記接続装置の前記パスワードコントローラは、前記選択時間に応じてパスワードを選択する。

【0018】

さらに、前記パスワードコントローラは、時間に応じて複数のパスワード生成アルゴリズムの中から1つを選択し、該パスワード生成アルゴリズムによりパスワードを生成する。

【0019】

【発明の実施の形態】

次に本発明の認証システムの第 1 の実施の形態について図面を参照して説明する。

【 0 0 2 0 】

図 1 を参照すると、本発明の第 1 の実施の形態は、ネットワーク 4 に接続された接続装置 1 と、この接続装置 1 に接続される複数の端末 2 によって構成される。接続装置 1 と各端末 2 とはそれぞれ伝送媒体 3 で接続され、既知の標準化団体 IEEE802.3 で規定されるアクセス方式（CSMA/CD 方式）等に従ってフレームの送受信が行われる。また、接続装置 1 は、ネットワーク 4 を介して他の接続装置 1 と相互に接続されており、各端末間の通信を制御する。

【 0 0 2 1 】

尚、接続装置 1 として、例えば、ハブやスイッチなど等を使用することができる。

【 0 0 2 2 】

また、接続装置 1 は、パスワードの生成を行うパスワードコントローラ 1 1、パスワードの比較を行うパスワード比較器 1 2、ネットワーク 4 とフレームの送受信を行うフレーム転送処理部 1 3、および、1 つ以上のインタフェース 1 4 を有して構成される。

【 0 0 2 3 】

端末 2 は、パスワードの生成を行うパスワードコントローラ 2 1、接続装置 1 とフレームの送受信を行うフレーム送受信部 2 2 および送信するフレームの組立を行うフレーム組立部 2 3 を有して構成される。

【 0 0 2 4 】

パスワードコントローラ 1 1 は、パスワードを複数保持しており、時刻にしたがって複数のパスワードの中から所定のパスワードを選択して出力する機能を有している。また、パスワードコントローラ 2 1 もパスワードコントローラ 1 1 と同様の構成である。

【 0 0 2 5 】

パスワード比較器 1 2 は、インタフェース 1 4 から送られてくる送信フレームのパスワードと、接続装置 1 内のパスワードコントローラ 1 1 で選択されたパス

ワードとを比較する。

【 0 0 2 6 】

フレーム転送処理部 1 3 は、ネットワーク 4 とのフレームの送受信などを行う。

【 0 0 2 7 】

また、フレーム組立部 2 3 は、接続装置 1 に送出すべきフレームにパスワードを付加する。図 2 を参照すると、フレーム組立部 2 3 は、パスワードコントローラ 2 2 で選択されたパスワードを、宛先アドレス、送信元アドレスおよびデータ部の先頭に付加してフレーム 5 を組み立てる。

【 0 0 2 8 】

次に、本発明の接続装置 1 の各構成要素およびその動作について図面を用いてさらに詳細に説明する。

【 0 0 2 9 】

図 3 を参照すると、接続装置 1 のインタフェース 1 4 は、フレームを端末と伝送媒体 3 を介して送受信するためのフレーム制御部 1 4 1 と、フレーム制御部 1 4 1 によって受信されたフレームを一時的に保持しておくフレームバッファ 1 4 2 とを有して構成されている。

【 0 0 3 0 】

また、パスワードコントローラ 1 1 は、タイマ 1 1 1、アルゴリズム格納メモリ 1 1 2、設定メモリ 1 1 3、パスワード選択回路 1 1 4 を有して構成されている。タイマ 1 1 1 は、接続装置 1 における現在時刻を指し示す。パスワード格納メモリ 1 1 2 は、複数種のパスワードを格納している。設定メモリ 1 1 3 は、図 4 に示されるように、時刻によっていずれのパスワードを使用するかを示す設定情報 6 を格納している。パスワード選択回路 1 1 4 は、タイマ 1 1 1 および設定メモリ 1 1 3 の内容によりパスワード格納メモリ 1 1 2 から該当するパスワードを選択する。

【 0 0 3 1 】

図 5 を参照すると、まず、接続装置 1 のフレーム制御部 1 4 1 は、端末 2 が接続装置 1 に接続されているか否かを判断する (S 1 1) 。端末 2 の接続が確認さ

れると、フレーム制御部141は、パスワードコントローラ11のタイマ111から接続装置1の現在時刻を讀出し、端末2へと送信する(S12)。その後、端末2からフレームが送信されてくるか否かを監視する(S13)。端末2からフレームが送信されてくると、フレーム制御部141は、送信されてきたフレームに付加されたパスワードをパスワード比較器12へ、残りのフレーム部分をフレームバッファ142へと送信する(S14)。パスワード比較器12は、フレーム制御部141からのパスワードと、パスワード選択回路114で選択されたパスワードとを比較する(S15)。比較の結果、パスワードが一致していれば、フレーム制御部141はフレームバッファ142に保持されたフレームをフレーム転送処理部13へと転送する(S16)。一方、パスワードが一致しなければ、フレーム制御部141は、フレームバッファ142に保持されたフレームを廃棄し、端末2にネットワーク4へのアクセスが許可できない旨を通知する(S17)。

【0032】

次に、パスワードコントローラ11の動作について説明する。図6を参照すると、パスワードコントローラ11では、パスワード選択回路114は、まず、タイマ111から現在時刻を受け取り、設定メモリ113に格納される設定情報6を参照する(S21)。パスワード選択回路114は、パスワード格納メモリ112から使用すべきパスワードを讀出す(S22)。パスワード選択回路114は、讀出したパスワードをパスワード比較器12へ送出する(S23)。

【0033】

ここで、パスワード選択回路114は、選択するパスワードが前回と同じである場合は、パスワード格納メモリ112から逐次パスワードを讀込むことなく、前回選択したパスワードをそのままパスワード比較器12へ再送するような構成してもよい。

【0034】

また、本発明の端末2の各構成要素およびその動作について図面を用いてさらに詳細に説明する。

【0035】

図 7 を参照すると、端末 2 のパスワードコントローラ 2 1 は、接続装置 1 のパスワードコントローラ 1 1 と同様に構成されており、パスワード格納メモリ 2 1 2 および設定メモリ 2 1 3 には接続装置 1 のパスワード格納メモリ 1 1 2 および設定メモリ 1 1 3 と同一の内容が格納されている。また、パスワード選択回路 2 1 4 は、図 6 に示される接続装置 1 のパスワード選択回路 1 1 4 と同様に動作し、タイマ 2 1 1 および設定メモリ 2 1 3 の設定情報 6 から該当するパスワードをパスワード格納メモリからパスワードを選択する。唯一、端末 2 のタイマ 2 1 1 が接続装置 1 のタイマ 1 1 1 と異なる。すなわち、端末 2 のタイマ 2 1 1 は、端末 2 の現在時刻を保持するものではなく、端末 2 が接続装置 1 に接続された際に接続装置 1 から送信されてくる接続装置 1 のタイマ 1 1 1 が示す時刻が設定される。

【 0 0 3 6 】

次に、端末 2 のフレーム送受信部 2 2 の動作について説明する。図 8 を参照すると、端末 2 が接続装置 1 に接続されると、まず、端末 2 のフレーム送受信部 2 2 は、接続装置 1 から現在時刻を受け取る（S 3 1）。フレーム送受信部 2 2 は、接続装置 1 の現在時刻を受け取ると、端末 2 のタイマ 2 1 1 に時刻を設定し、接続装置 1 および端末 2 のタイマ 1 1 1 および 2 1 1 の同期を図る（S 3 2）。フレーム送受信部 2 2 は、タイマ 1 1 1 および 2 1 1 の同期を取った後、接続装置 1 に対してフレーム送信があれば（S 3 3）、図 3 に示されるパスワードが付加されたフレーム 5 をフレーム組立部 2 3 から受け取り、接続装置 1 へと送出する（S 3 4）。

【 0 0 3 7 】

さらに、端末 2 のフレーム組立部 2 3 の動作について説明する。図 9 を参照すると、フレーム組立部 2 3 は、図示せぬプロセッサからフレームの送信命令を受け取ると（S 4 1）、パスワード生成部 2 1 4 からパスワードを取得する（S 4 2）。フレーム組立部 2 3 は、フレーム組立部 2 3 は宛先アドレス、送信元アドレスおよびデータ部からなるフレームの先頭に取得したパスワードを付け加える（S 4 3）。そして、フレーム組立部 2 3 は、パスワードが付加されたフレーム 5 をフレーム送受信部 2 2 へ送出する（S 4 4）。

【 0 0 3 8 】

このように、本発明においては、パスワード生成回路で使用するパスワードを変化させる。したがって、あるパスワードが解読されるなどして漏洩した場合でも、本発明は時間の経過に伴ってパスワードが変更されるため不正アクセスを検出してネットワークへの接続を不許可にすることができ、ネットワークの高いセキュリティを実現できる。

【 0 0 3 9 】

次に、本発明の第 1 の実施の形態の動作について説明する。

【 0 0 4 0 】

図 1 および図 1 0 を参照すると、まず、接続装置 1 に端末 2 が接続されると、接続装置 1 のタイマ 1 1 1 が示す現在時刻を端末 2 へ送信する (S 1 0 1)。フレーム送受信部 2 2 は、送信された時刻をタイマ 2 1 1 に設定し、接続装置 1 と同期を図る (S 1 0 2)。端末 2 が、接続装置 1 に対してデータ送信やアクセス要求といったフレームの送信を行う場合には (S 1 0 3)、端末 2 のパスワードコントローラ 2 1 が、複数のパスワードの中から現在時刻によって決まるパスワードを選択する (S 1 0 4)。フレーム組立部 2 3 はパスワードコントローラ 2 1 で選択されたパスワードを付加したフレーム 5 を組立ててフレーム送受信部 2 2 へ送出する (S 1 0 5)。フレーム送受信部 2 2 は、パスワードが付加されたフレーム 5 を伝送媒体 3 を介して接続装置 1 へ送出する (S 1 0 6)。接続装置 1 のインタフェース 1 4 は、伝送媒体 3 を介して接続されている端末 2 からフレーム 5 を受け取ると、フレーム 5 からパスワードを読み出してパスワード比較器 1 2 へ送出する (S 1 0 7)。パスワードコントローラ 1 1 は、複数のパスワードの中から現在時刻によって決まるパスワードを選択する (S 1 0 8)。パスワード比較器 1 2 は、パスワードコントローラ 1 1 が選択したパスワードと、受信したフレーム 5 から読み出されたパスワードとを比較する (S 1 0 9)。比較の結果、パスワードが一致した場合、インタフェース 1 4 はフレーム 5 を送信してきた端末 2 がネットワーク 4 への通信 (アクセス) を許可されていると判断し、パスワードを除いたフレームをフレーム転送処理部 1 3 へ送出する (S 1 1 0)。一方、パスワードが一致しない場合、インタフェース 1 4 は端末 2 がネットワ

ーク 4 に不正アクセスしているものと判断し、フレーム転送を不許可として該フレームを廃棄して端末 2 に通知する（S 1 1 1）。

【 0 0 4 1 】

尚、パスワードが一致しない場合は、所定の回数だけ再送させる構成としてもよい。

【 0 0 4 2 】

以上のような構成により、不正に入手されたパスワードを用いて不正アクセスが行われたとしても、設定メモリ 1 1 3 に定められた時間によるパスワードの変化によって不正アクセスを発見することができ、よりセキュリティの高い認証システムを提供することが可能となる。

【 0 0 4 3 】

次に、本発明の認証システムの第 2 の実施の形態について図面を参照して説明する。

【 0 0 4 4 】

この第 2 の実施の形態においては、端末 2 のフレーム組立部 2 3 が、図 1 1 に示されるように、パスワードとともにそのパスワードが選択されたパスワード選択時間をフレーム 7 に付加する構成とする。また、接続装置 1 では受け取ったフレーム 7 のパスワード選択時間に従ってパスワードを選択する構成とする。これにより、接続装置 1 と端末 2 との間で発生するパスワード選択時間の時間差を無くすことができ、的確なパスワードの比較が行えるようになる。

【 0 0 4 5 】

接続装置 1 のフレーム制御部 1 4 1 は、端末 2 からフレーム 7 を受け取ると、フレーム 7 のパスワードをパスワード比較器 1 2 に、パスワード選択時間をパスワード選択回路 1 1 4 に、その他の残りの部分をフレームバッファ 1 4 2 に送信する点のみが第 1 の実施の形態における動作と異なる。その他の動作については図 6 に示される第 1 の実施の形態の動作と同様である。

【 0 0 4 6 】

しかしながらこのような構成の場合、パスワードが漏洩した際に端末 2 から現在時刻を偽ってアクセスされた場合、これを防止することができなくなってしまう

う。そこで、このことを考慮して、接続装置 1 の現在時刻と所定時間以上離れたパスワード選択時間は採用しない構成とする。

【0047】

図 1 2 を参照すると、接続装置 1 のパスワードコントローラ 1 1 は、有効時間格納メモリ 1 1 5 をさらに有する。この有効時間格納メモリは、パスワード選択時間を有効と判定する有効時間を格納している。

【0048】

以下に本発明の第 2 の実施の形態のパスワードコントローラ 1 1 の動作を説明する。

【0049】

図 1 3 を参照すると、まず、パスワード選択回路 1 1 4 は、フレーム制御部 1 4 1 からパスワード選択時間を受けると (S 5 1)、受け取ったパスワード選択時間とタイマ 1 1 1 の示す現在時刻との時間差が有効時間格納メモリ 1 1 5 に格納された有効時間以内であるか否かを判定する (S 5 2)。もし、パスワード選択時間とタイマの示す現在時刻との差が有効時間以内であれば、パスワード選択回路 1 1 4 はパスワード選択時間および設定メモリ 1 1 3 の内容から使用すべきパスワードを選択する (S 5 3)。一方、パスワード選択時間とタイマの示す現在時刻との差が有効時間以上であれば、パスワード選択回路 1 1 4 はパスワード選択時間を採用せず、タイマ 1 1 1 の示す現在時刻と設定メモリ 1 1 3 の内容から使用すべきパスワードを選択する (S 5 4)。パスワード選択回路 1 1 4 は、選択したパスワードをフレーム比較器 1 2 へ送出する (S 5 5)。

【0050】

このような構成により、アルゴリズムが変更される時間の前後における通信においても、接続装置 1 および端末で異なるパスワードが用いられてパスワードが不一致となることがなくなり、的確なパスワードの比較が実現されることになる。

【0051】

さらに、本発明の認証システムの第 3 の実施の形態について図面を参照して説明する。

【0052】

この本発明の第3の実施の形態では、第1の実施の形態におけるパスワードコントローラ11および21の構成およびその動作が異なる。その他の構成要素およびそれらの動作については第1の実施の形態と同様である。以下、接続装置1のパスワードコントローラ11について説明するが、端末2のパスワードコントローラ21も同様である。

【0053】

図14を参照すると、第3の実施の形態におけるパスワードコントローラ11は、複数のパスワードを格納するパスワード格納メモリ112に変えて、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリ116を設ける。また、パスワード選択回路114に変えて、アルゴリズム格納メモリ116から1つのパスワード生成アルゴリズムを読み出してパスワードを生成するパスワード生成回路117を設ける。さらに、設定メモリ113には、図15に示されるようにパスワード生成回路117がパスワード生成アルゴリズムを使用する時間を規定する設定情報8を保持する。

【0054】

尚、パスワード生成アルゴリズムとしては、分単位程度の時間をパラメータとする一般的な数学による方程式等を利用すればよい。

【0055】

以下に、本発明の第3の実施例におけるパスワードコントローラ11の動作について図面を参照して説明する。尚、複数のパスワード生成アルゴリズムは、それぞれ分単位の時間をパラメータとする方程式であるとする。

【0056】

図14および図16を参照すると、まず、パスワード生成回路117は、タイマ111の現在時刻および設定メモリ113の設定情報8を参照して使用するパスワード生成アルゴリズムをアルゴリズム格納メモリ116から選択する(S61)。パスワード生成回路117は、選択したパスワード生成アルゴリズムを使用し、タイマ111の現在時刻をパラメータとしてパスワードを生成する(S62)。その後、パラメータが変化(時刻の分単位が変化)すると(S63)、設

定情報 8 を参照して使用するアルゴリズムが変更になったか否かを確認する (S 6 4)。使用するアルゴリズムが変更された場合は、変更されたパスワード生成アルゴリズムをアルゴリズム格納メモリ 1 1 6 から選択し (S 6 5)、タイマ 1 1 1 の現在時刻をパラメータとしてパスワードを生成する (S 6 2 へ)。一方、使用するアルゴリズムに変更がなければ、パスワード生成回路 1 1 7 は新たなパラメータ (時刻) を用いてパスワードを再生成する (S 6 2 へ)。

【0 0 5 7】

また、さらに、第 3 の実施の形態に対して、第 2 の実施の形態で示したパスワード選択時間にかえて、パスワードを生成した時間をパスワード生成時間としてフレームに付加する構成としてもよい。

【0 0 5 8】

以上のように、本発明においては、各端末 2 が接続装置 1 に接続された際に接続装置 1 の時刻と同期が取られ、この時刻に合わせてパスワードが変化することになる。したがって、接続装置 1 と同一のパスワード (または、アルゴリズム) および設定情報を有している正当な端末であれば、接続装置 1 が時間の経過とともにパスワードを変化させても、接続装置 1 と同様にパスワードを変化させることができる。よって、設定メモリ 1 1 3 および 2 1 3 に設定に合わせて異なるパスワードを用いて通信を続行することが可能となる。これに対し、不正に入手したパスワードを利用して通信を行った場合には、時間に伴う接続装置 1 のパスワードの変化によってパスワード比較器 1 2 がパスワードの不一致を検出し、不正アクセスが発見されることになる。

【0 0 5 9】

【発明の効果】

以上の説明で明らかなように、本発明によると、正しいパスワードをフレームに含めて送信できない端末は、接続装置内でフレームを廃棄する。このため、不正な他端末は他の端末との通信が成立しなくなり、ネットワークセキュリティを保つことが可能になる。また、時間の経過とともにパスワードが変更されるため、アナライザ等によってある時点でパスワードが盗まれた (または、解析された) 場合においても、盗まれた (解析された) パスワードで継続的に接続装置を介

して通信が行われることを防止することができる。

【図面の簡単な説明】

【図 1】

本発明の認証システムの実施の形態を示すブロック図である。

【図 2】

本発明で使用されるフレームの構成を示す図である。

【図 3】

本発明の接続装置の実施の形態を示す図である。

【図 4】

本発明の設定メモリに格納される設定情報を示す図である。

【図 5】

本発明の接続装置のフレーム制御部の動作を説明する流れ図である。

【図 6】

本発明の接続装置のパスワードコントローラの動作を説明する流れ図である。

【図 7】

本発明の端末の実施の形態を示す図である。

【図 8】

本発明の端末のフレーム送受信部の動作を説明する流れ図である。

【図 9】

本発明の端末のフレーム組立部の動作を説明する流れ図である。

【図 1 0】

本発明の認証システムの動作を説明する流れ図である。

【図 1 1】

本発明の第 2 の実施の形態で使用するフレームの構成を示す図である。

【図 1 2】

本発明の第 2 の実施の形態におけるパスワードコントローラの構成を示す図である。

【図 1 3】

本発明の第 2 の実施の形態におけるパスワードコントローラの動作を説明する

流れ図である。

【図 1 4】

本発明の第 3 の実施の形態におけるパスワードコントローラの構成を示す図である。

【図 1 5】

本発明の第 3 の実施の形態における設定メモリに格納される設定情報を示す図である。

【図 1 6】

本発明の第 3 の実施の形態におけるパスワードコントローラの動作を説明する流れ図である。

【図 1 7】

従来のシステムの概略を示すブロック図である。

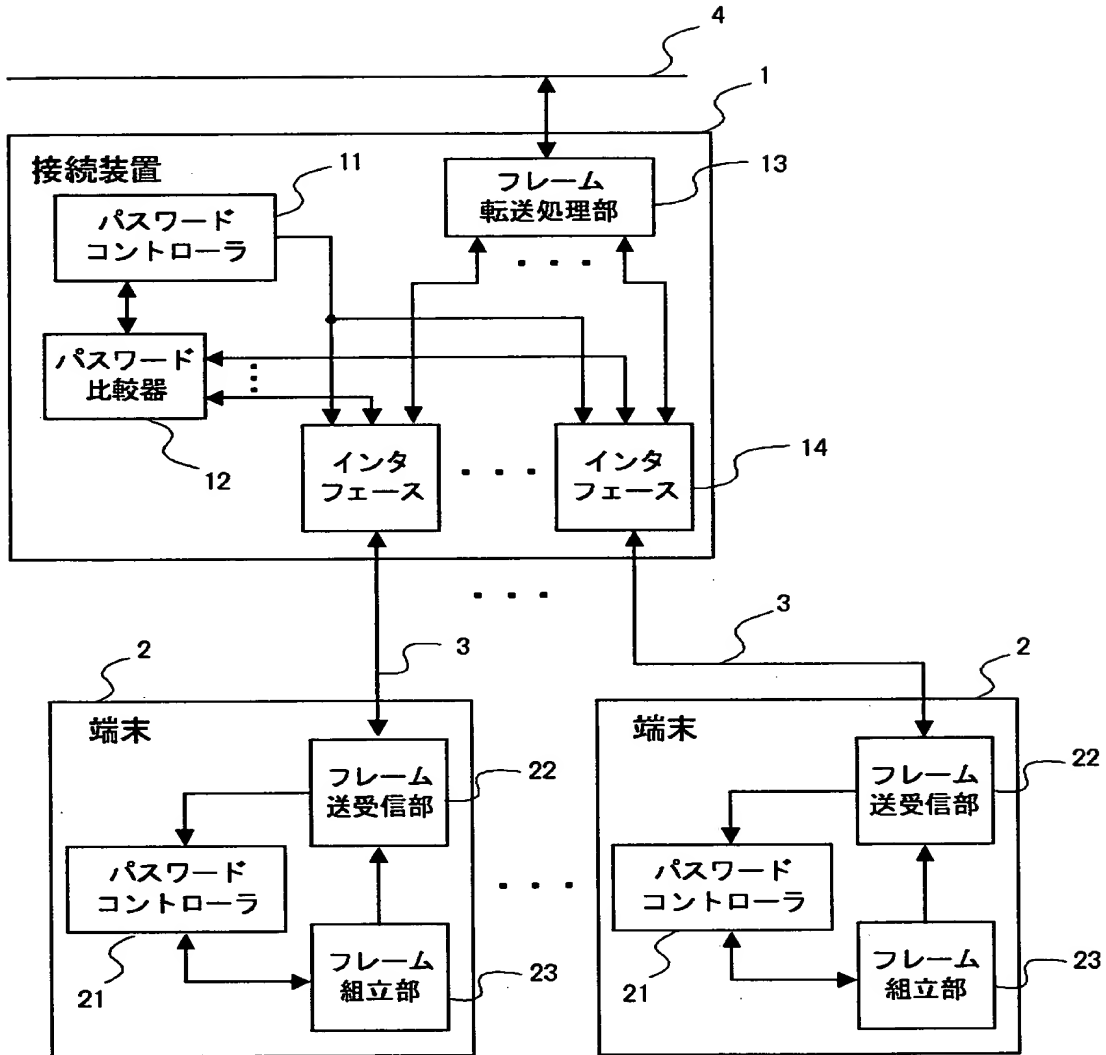
【符号の説明】

- 1 接続装置
- 2 端末
- 3 伝送媒体
- 4 ネットワーク
- 5、7 フレーム
- 6、8 設定情報
- 1 1、2 1 パスワードコントローラ
- 1 2 パスワード比較器
- 1 3 フレーム転送処理部
- 1 4 インタフェース
- 2 2 フレーム送受信部
- 2 3 フレーム組立部
- 1 1 1、2 1 1 タイマ
- 1 1 2、2 1 2 パスワード格納メモリ
- 1 1 3、2 1 3 設定メモリ
- 1 1 4、2 1 4 パスワード選択回路

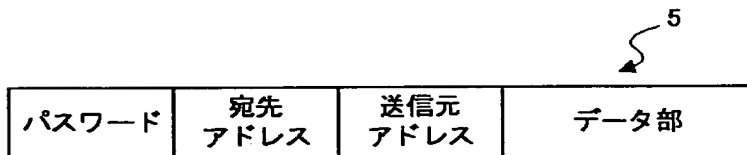
- 1 1 5 判定条件格納メモリ
- 1 1 6 アルゴリズム格納メモリ
- 1 1 7 パスワード生成回路
- 1 4 1 フレーム制御部
- 1 4 2 フレームバッファ

【書類名】 図面

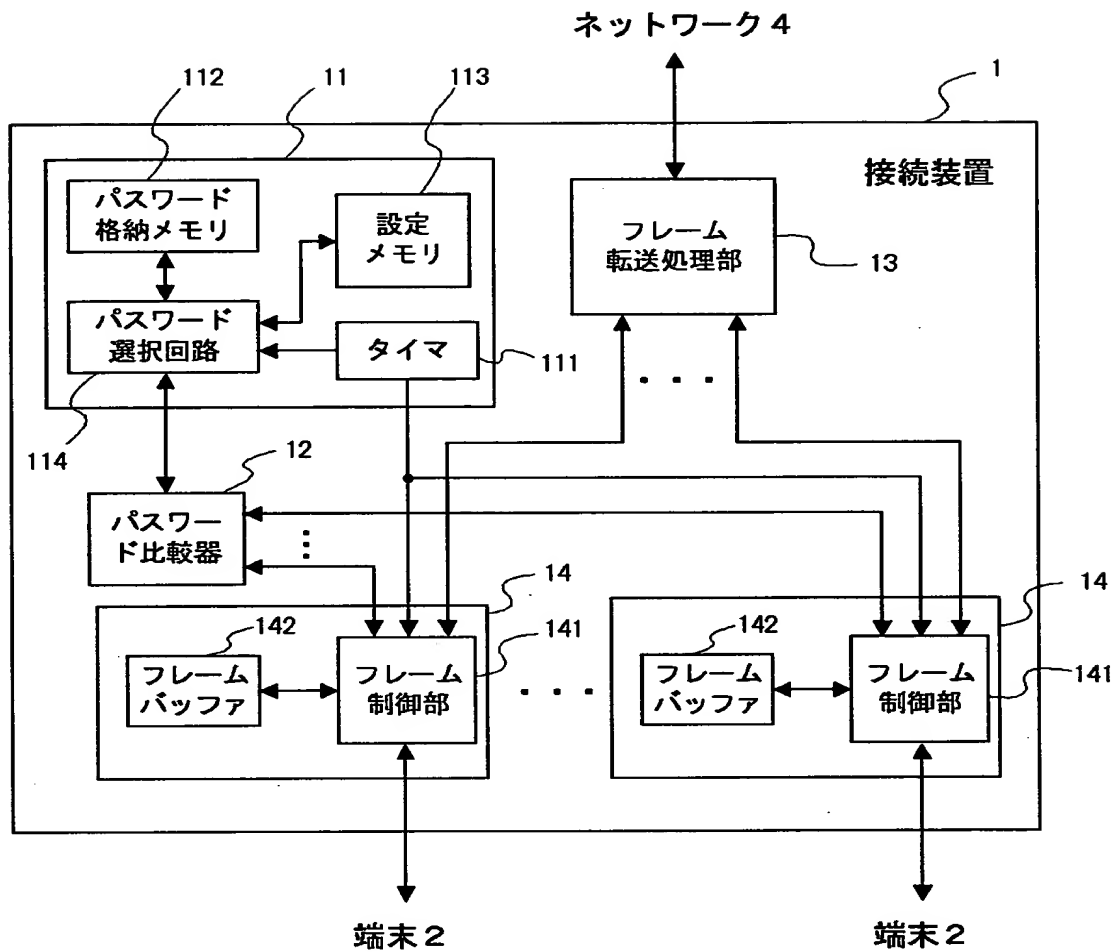
【図 1】



【図 2】



【図3】

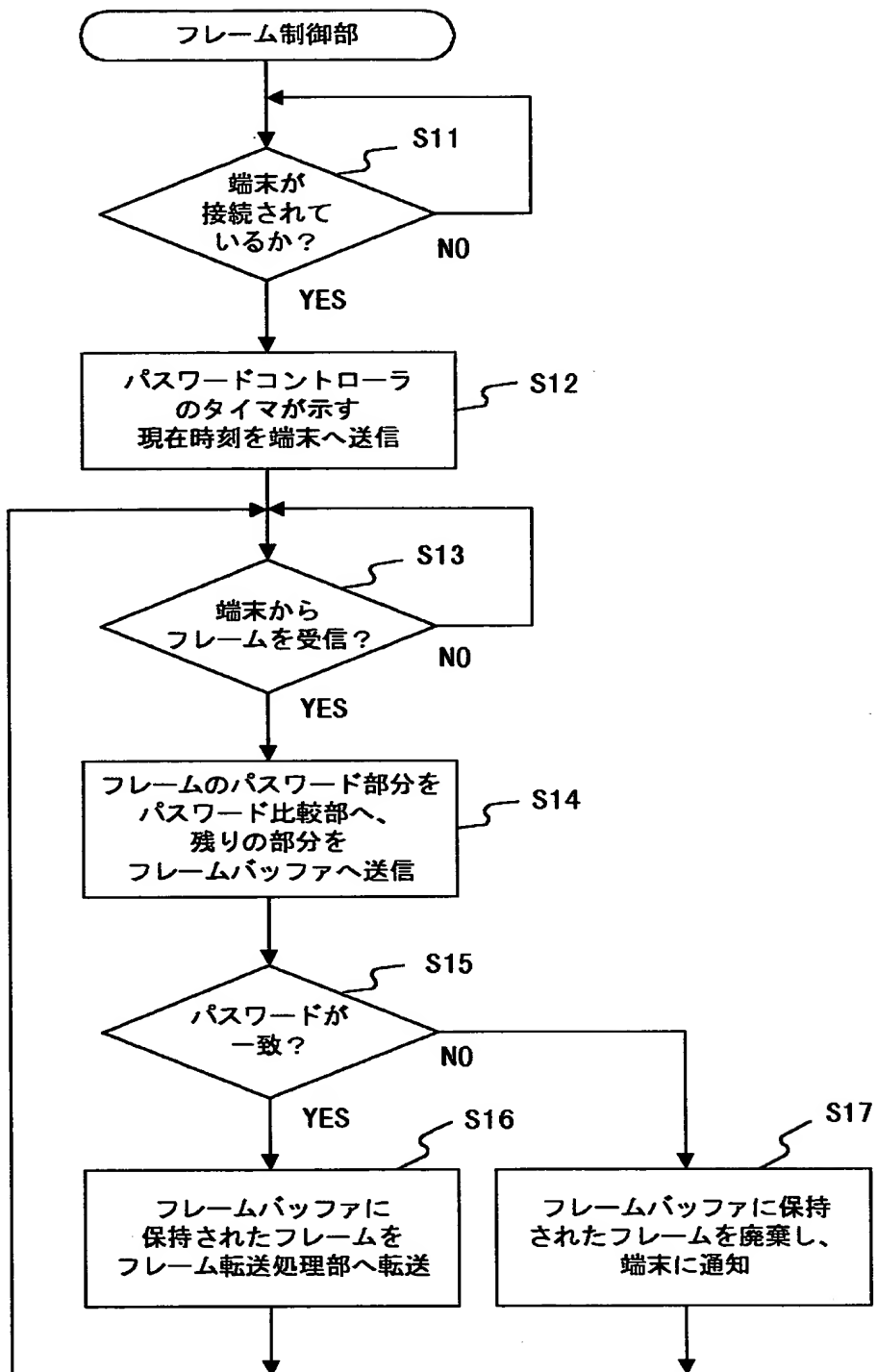


【図4】

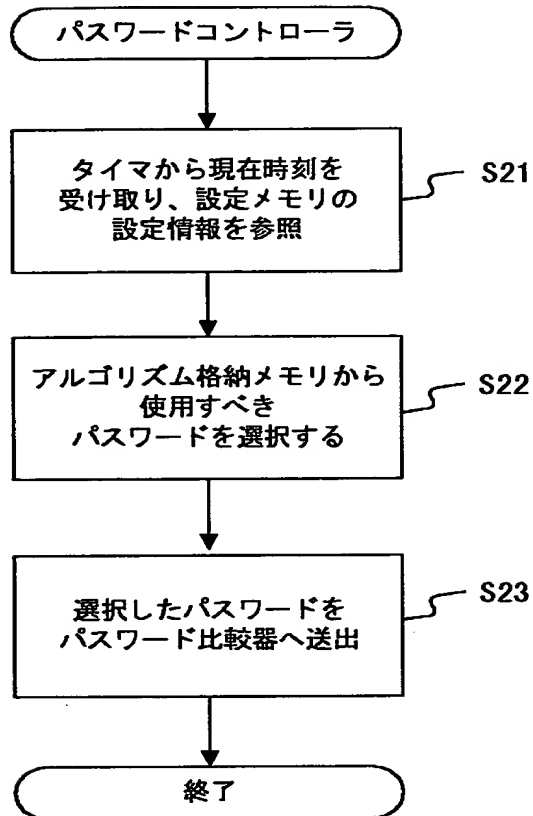
6

時間	使用するパスワード
0:00-0:04	パスワードA
0:05-0:10	パスワードB
⋮	⋮
23:55-23:59	パスワードX

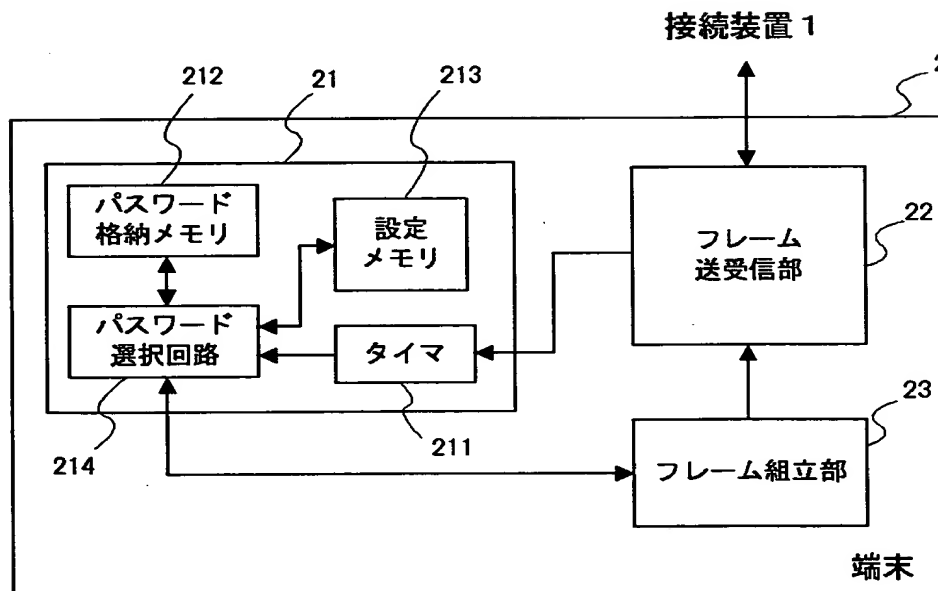
【図 5】



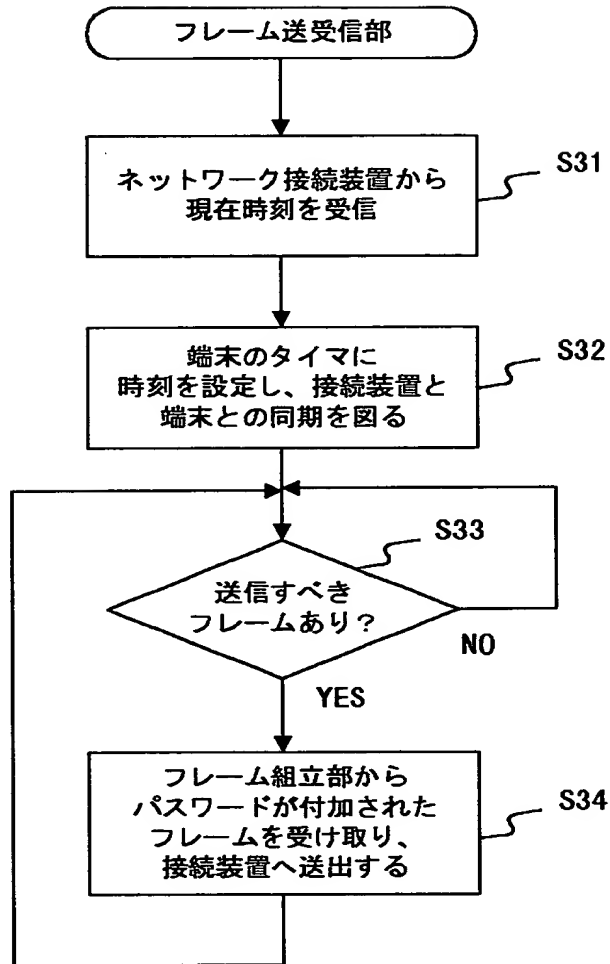
【図 6】



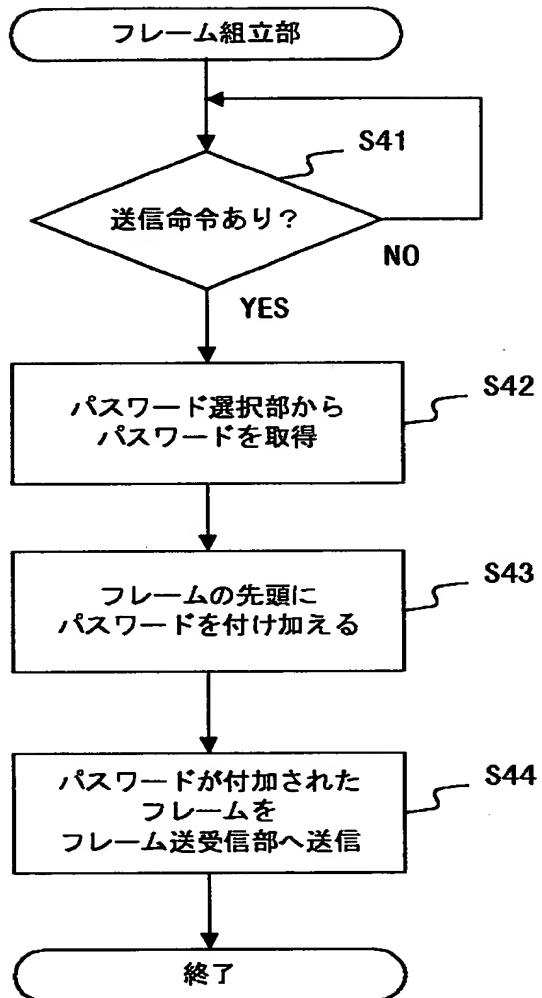
【図 7】



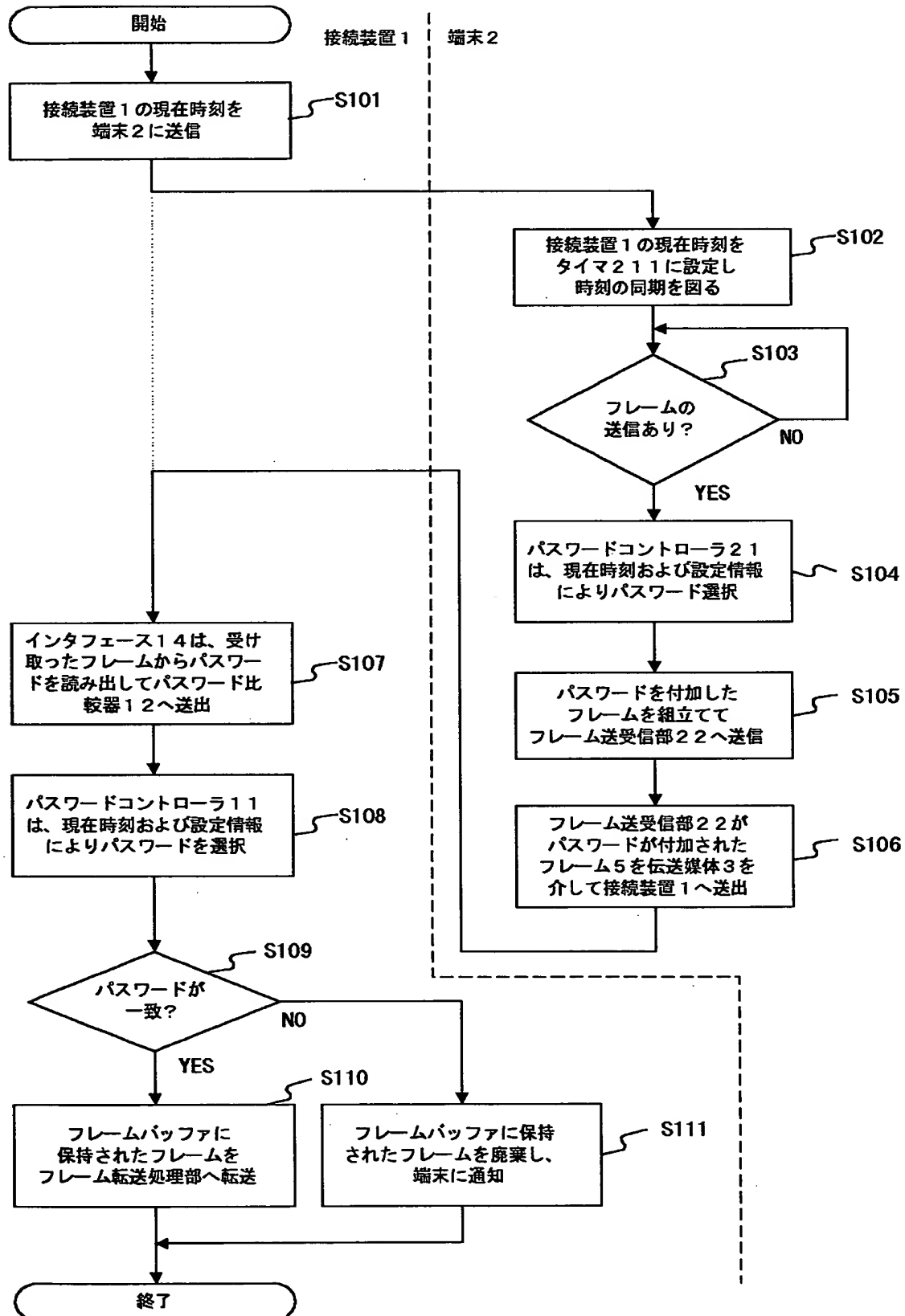
【図 8】



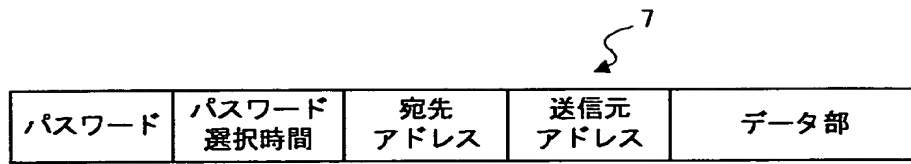
【図 9】



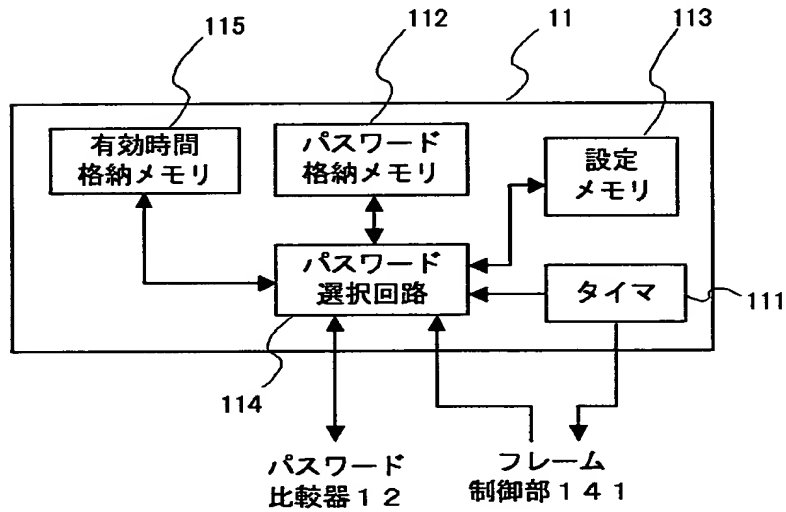
【図10】



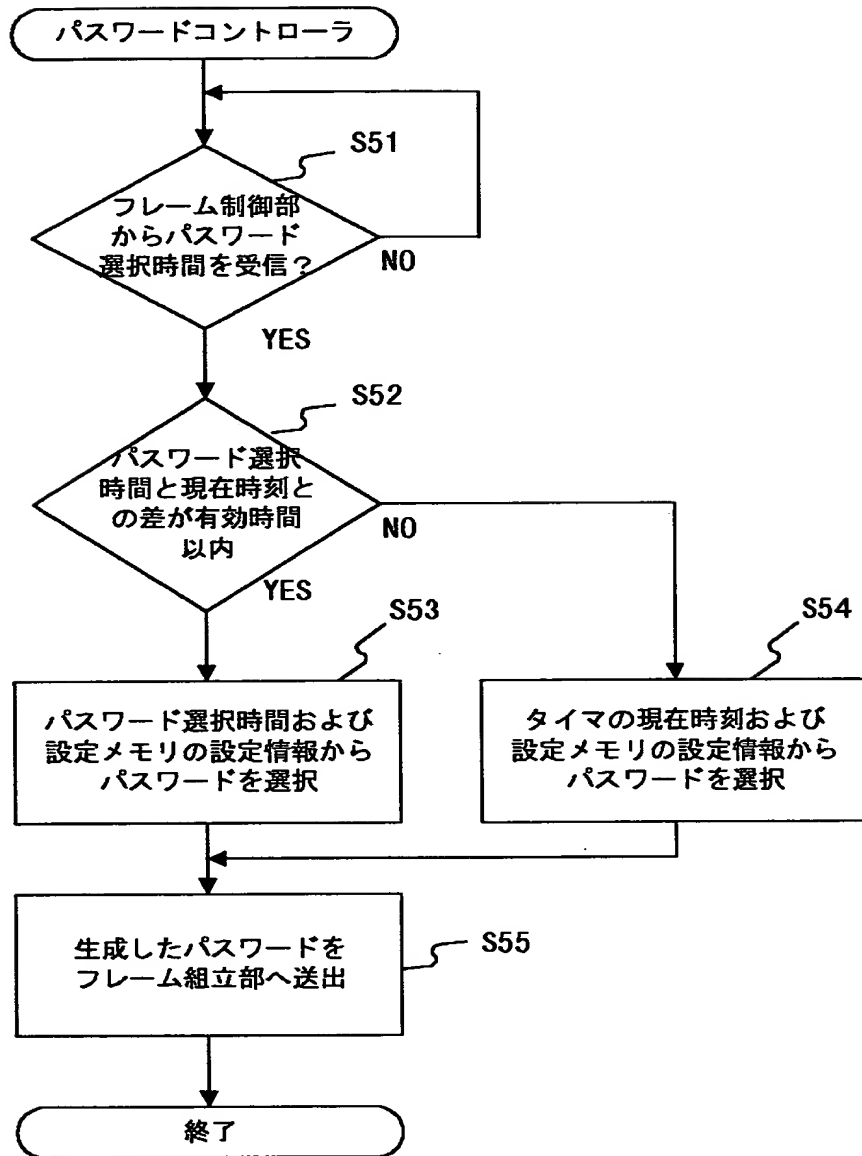
【図 1 1】



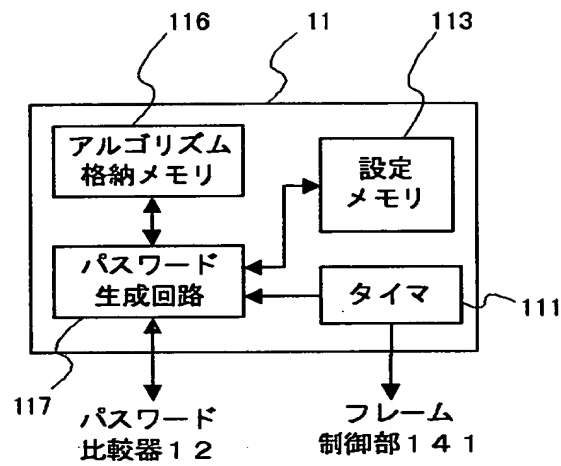
【図 1 2】



【図 13】



【図 1 4】

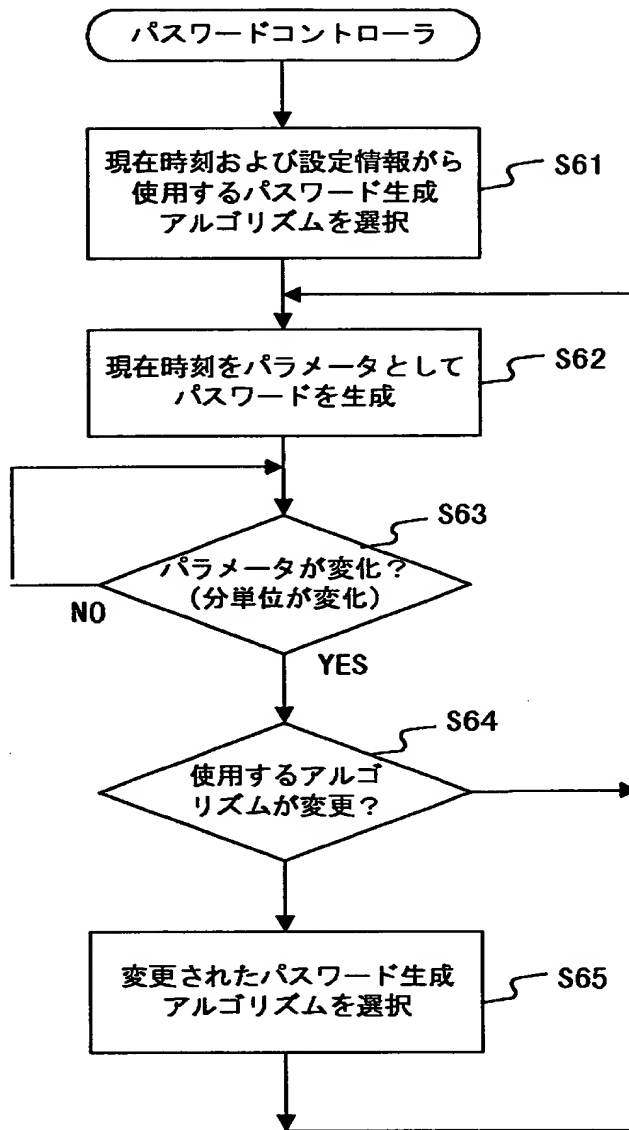


【図 1 5】

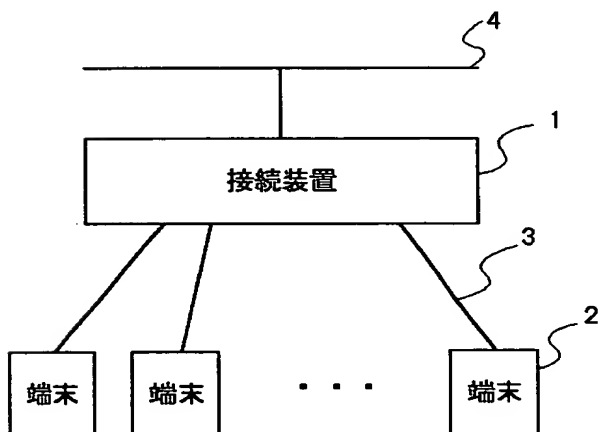
8

時間	使用するアルゴリズム
0:00-0:04	アルゴリズム A
0:05-0:10	アルゴリズム B
⋮	⋮
23:55-23:59	アルゴリズム X

【図 16】



【図 17】



特2000-015670

【書類名】 要約書

【要約】

【課題】 送信元アドレスやパスワードの盗用による不正アクセスを検出して排除できるセキュリティの高い認証システムを提供する。

【解決手段】 接続装置 1 および端末 2 のそれぞれに複数のパスワード（または複数のパスワード生成アルゴリズム）および設定情報を格納する。接続装置 1 と端末 2 との時刻を同期させ、設定情報により時間の経過とともにパスワード（またはパスワード生成アルゴリズム）を変更してパスワードを変化させる。端末 2 は送信するフレームにパスワードを付加して送出し、接続装置 1 は受け取ったフレームのパスワードと接続装置 1 のパスワードとを比較する。パスワードが一致した場合、接続装置 1 は端末 2 の通信を許可し、一致しない場合には通信を不許可としてフレームを廃棄する。

【選択図】 図 1

特2000-015670

認定・付加情報

特許出願の番号	特願2000-015670
受付番号	50000071002
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 1月26日

<認定情報・付加情報>

【提出日】	平成12年 1月25日
-------	-------------

次頁無

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社